

#3

PATENT
83308.0001
JC928 U.S. PRO
09/726180
11/29/00

Express Mail Label No. EL 589 806 213 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Masao KASAHARA

Serial No: Not assigned

Filed: November 29, 2000

For: A CRYPTOSYSTEM USING
MULTIVARIABLE POLYNOMIALS

Art Unit: Not assigned

Examiner: Not assigned

TRANSMITTAL OF PRIORITY DOCUMENTBox PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-066226 which was filed March 10, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: November 29, 2000

By: Louis A. Mok
Registration No. 22,585
Attorney for Applicant(s)500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

JC928 U.S. PRO
09/726180
11/29/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

2000年 3月10日

願 番 号
Application Number:

特願2000-066226

願 人
Applicant(s):

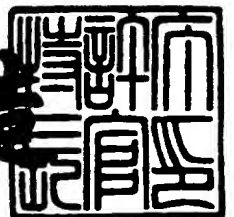
村田機械株式会社
笠原 正雄

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 7月28日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2000-3060263

【書類名】 特許願

【整理番号】 MF0001

【特記事項】 特許法第 3 0 条第 1 項の規定の適用を受けようとする特
許出願

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 9/00

【発明者】

 【住所又は居所】 大阪府箕面市粟生外院 4 丁目 1 5 番 3 号

 【氏名】 笠原 正雄

【特許出願人】

 【識別番号】 000006297

 【氏名又は名称】 村田機械株式会社

【特許出願人】

 【識別番号】 597008636

 【氏名又は名称】 笠原 正雄

【代理人】

 【識別番号】 100086830

 【弁理士】

 【氏名又は名称】 塩入 明

【選任した代理人】

 【識別番号】 100096046

 【弁理士】

 【氏名又は名称】 塩入 みか

【手数料の表示】

 【予納台帳番号】 012047

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

 【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9804018

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 復号方法、復号装置、及び復号プログラムの記録媒体

【特許請求の範囲】

【請求項 1】 デジタル情報処理装置を用いて、素体の有限次元拡大体の元として表現された暗号を復号する方法において、前記暗号に第 1 の秘密鍵を乗算するステップと、第 2 の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するステップ、とを有することを特徴とする、復号方法。

【請求項 2】 第 1 の秘密鍵を、前記有限次元拡大体の原始多項式の原始根のべき乗とすることを特徴とする、請求項 1 の復号方法。

【請求項 3】 第 2 の秘密鍵で分離したメッセージ対応部に、第 3 の秘密鍵の多項式を乗算することを特徴とする、請求項 1 または 2 の復号方法。

【請求項 4】 第 4 の秘密鍵を用いてべき乗根を求めるステップを付加したことを特徴とする、請求項 3 の復号方法。

【請求項 5】 デジタル情報処理装置で、素体の有限次元拡大体の元として表現された暗号を復号するために、情報ネットワークを介して、前記暗号に第 1 の秘密鍵を乗算するステップと、第 2 の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するステップとを実行させるためのプログラムを、前記デジタル情報処理装置に送信して、該デジタル情報処理装置で暗号を復号させることを特徴とする、復号方法。

【請求項 6】 素体の有限次元拡大体の元として表現された暗号を復号するために、前記暗号に第 1 の秘密鍵を乗算するための乗算手段と、第 2 の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するための置換手段、とを備えた復号装置。

【請求項 7】 前記乗算手段を、前記有限次元拡大体の原始多項式の原始根のべき乗を暗号に乗算するように構成すると共に、前記置換手段で分離したメッセージ対応部に、第 3 の秘密鍵の多項式を乗算しかつ第 4 の秘密鍵を用いてべき乗根を求めるための手段を設けたことを特徴とする、請求項 6 の復号装置。

【請求項 8】 素体の有限次元拡大体の元として表現された暗号を復号するために、前記暗号に第 1 の秘密鍵を乗算するステップと、第 2 の秘密鍵で暗号内で

の要素の順序を置換してメッセージ対応部とノイズとに分離するステップとを、デジタル情報処理装置に実行させるためのプログラムを記憶した、デジタル情報処理装置で読み出し可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の利用分野】

この発明は暗号システムや暗号通信に関し、特に多変数の多項式の求解困難性を利用した暗号システムや暗号通信に関する。

【0002】

【従来技術】

多変数の多項式を用いた暗号が提案されている(例えば、Matsumoto et al, Public Quadatic Polynomial - tuples for Efficient Signature Verification and Message-encryption, Proc. of EUROCRYPT 88, Springer Verlag, Vol.20, P.P.419-453)。このような暗号では、ガロワ体の元を多項式で表現し、多項式の各次元の係数に、メッセージをコーディングする。そしてメッセージの各要素を変数と見なすと、前記の係数は多変数の多項式となる。しかしながら多変数の多項式を用いた暗号の安全性は確認されておらず、発明者は多変数多項式を用いた暗号の安全性を高めることを検討して、この発明に到った。

【0003】

【発明の課題】

この発明の基本的課題は、多変数多項式を用いた強固な暗号技術を提供して、これを復号できるようにすることにある(請求項1～8)。

請求項2～4の発明の追加の課題は、復号化の具体的な方法を提供することにある。

請求項5の発明の追加の課題は、情報ネットワークを介して、復号プログラムを配信し、容易に暗号通信を行えるようにすることにある。

請求項6, 7の発明の追加の課題は復号装置を提供することであり、特に請求項7の発明の課題は復号装置の具体的な構成を提供することにある。

請求項 8 の発明の追加の課題は、復号プログラムを記憶した媒体を提供することにある。

【 0 0 0 4 】

【発明の構成】

この発明は、デジタル情報処理装置を用いて、素体の有限次元拡大体の元として表現された暗号を復号する方法において、前記暗号に第 1 の秘密鍵を乗算するステップと、第 2 の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するステップ、とを有することを特徴とする（請求項 1）。デジタル情報処理装置には、コンピュータの他に、暗号化や復号のための論理回路を組み込んだチップなどが含まれる。この発明で復号すべき暗号は、素体の有限次元拡大体の元であり、多項式表現での各次元の係数などに、メッセージの各要素が多変数多項式としてコーディングされたものである（請求項 1 ～ 8）。

【 0 0 0 5 】

好ましくは、第 1 の秘密鍵を、前記有限次元拡大体の原始多項式の原始根のべき乗とする。

また好ましくは、第 2 の秘密鍵で分離したメッセージ対応部に第 3 の秘密鍵の多項式を乗算する。

最も好ましくは、第 3 の秘密鍵の多項式の乗算しかつ第 4 の秘密鍵を用いてべき乗根を求める。多項式の乗算とべき乗根を求める順序はどちらが先でも良いが、好ましくは先に多項式を乗算し、次いでべき乗根を求める。

【 0 0 0 6 】

またこの発明は、デジタル情報処理装置で、素体の有限次元拡大体の元として表現された暗号を復号するために、情報ネットワークを介して、前記暗号に第 1 の秘密鍵を乗算するステップと、第 2 の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するステップ、とを実行させるためのプログラムを、前記デジタル情報処理装置に送信して、該デジタル情報処理装置で暗号を復号させる復号方法にある（請求項 5）。

この復号方法では最も好ましくは、第 1 の秘密鍵を、前記有限次元拡大体の原始多項式の原始根のべき乗とし、第 2 の秘密鍵で分離したメッセージ対応部に第

3 の秘密鍵の多項式を乗算し、第 3 の秘密鍵の多項式の乗算しかつ第 4 の秘密鍵でべき乗根を求めて復号する。

【 0 0 0 7 】

またこの発明は、素体の有限次元拡大体の元として表現された暗号を復号するために、前記暗号に第 1 の秘密鍵を乗算するための乗算手段と、第 2 の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するための置換手段、とを備えた復号装置にある（請求項 6）。

好ましくは、前記乗算手段を、前記有限次元拡大体の原始多項式の原始根のべき乗を暗号に乗算するように構成すると共に、前記置換手段で分離したメッセージ対応部に、第 3 の秘密鍵の多項式を乗算しかつ第 4 の秘密鍵でべき乗根を求めるための手段を設ける。

【 0 0 0 8 】

またこの発明は、素体の有限次元拡大体の元として表現された暗号を復号するために、前記暗号に第 1 の秘密鍵を乗算するステップと、第 2 の秘密鍵で暗号内での要素の順序を置換してメッセージ対応部とノイズとに分離するステップとを、デジタル情報処理装置に実行させるためのプログラムを記憶した、デジタル情報処理装置で読み出し可能な記録媒体にある（請求項 8）。

【 0 0 0 9 】

【発明の作用と効果】

発明者は、素体の有限次元拡大体上の多変数多項式を用いた、新規な暗号技術を開発した。この暗号技術では例えば、

- 1) メッセージと多項式とを乗算して多項式の係数にメッセージの各要素をコーディングすること、
- 2) メッセージにノイズを付加して対称群の元を作用させノイズとメッセージとをシャッフルすること、
- 3) メッセージに有限次元拡大体の元を乗算すること、

の 3 つの要素を用いる。そして実用的には少なくとも、メッセージにノイズを付加して置換群（対称群）の元を作用させた後、メッセージに拡大体の元を乗算して、拡大体の元の多項式表現での各次元にメッセージとノイズとを混合してコー

ディングすればよい。上記の暗号化を実際に行うには、暗号化のアルゴリズムを伏せて、単に暗号の各要素をメッセージの多項式と見なして、メッセージの値を上記の多項式に代入すればよい。このようにして得られた暗号は強度が高い。例えば、有限次元拡大体上でメッセージに多項式を乗算して、拡大体の元を多項式表現すると、各次元の係数はメッセージの複数の要素が入り交じった多変数の多項式となる。しかしながら、多項式とメッセージとの乗算のみでは、暗号の安全性は確認されていない。

【0010】

上記の多変数多項式の暗号に、ノイズの付加とノイズとメッセージとのシャッフルとを加えると、暗号を破ることは著しく困難となる。さらに、ノイズとメッセージとのシャッフルの後に、拡大体の元の乗算等を加えると、暗号を破るのはさらに困難になる。このようにして、強度が改善された暗号システムが得られる。この暗号システムでは、暗号化の過程では、暗号システムの特徴は余り表れない。暗号を復号する過程で、暗号化のアルゴリズムに対応した処理が表れ、復号に必要な処理は暗号化の処理の裏返しである。そこで上記の暗号システムを実用化するには、復号方法や復号装置等を提供する必要がある。

【0011】

この発明では、メッセージを素体の有限次元拡大体の元と見なす。以下では、有限次元拡大体を拡大体、あるいは単に体と呼ぶことがある。そしてメッセージを多項式の不定元に代入した暗号に対して、第1の秘密鍵（有限次元拡大体の元）の乗算と、第2の秘密鍵での暗号内の要素の置換による、メッセージ対応部とノイズとの分離を行う（請求項1）。この暗号を破るには、第1の秘密鍵と第2の秘密鍵が必要で、いずれも秘密鍵の候補は極めて多く、かつ第1の秘密鍵での乗算には有限次元拡大体を生成した既約多項式等を知る必要がある。この発明では、安全な暗号システムが得られる（請求項1～8）。

【0012】

請求項2の発明では、第1の秘密鍵を前記有限次元拡大体の原始多項式の原始根のべき乗とする。このため第1の秘密鍵は、べきの値を変えることにより、極めて広い範囲から選ぶことができ、安全性が高い。また原始根のべき乗は乗算

が簡単で、復号が容易である。

【0013】

請求項3の発明では、第2の秘密鍵で分離したメッセージ対応部に、第3の秘密鍵の多項式を乗算する。復号には、第1の秘密鍵との乗算、第2の秘密鍵での置換操作、第3の秘密鍵の多項式との乗算が必要で、仮に第3の秘密鍵を入手しても、ノイズを除いた有限次元拡大体の生成に用いた既約多項式等を知らなければ多項式との乗算ができず、暗号の信頼性が極めて高い。

【0014】

請求項4の発明では、第3の秘密鍵の多項式の乗算しかつ第4の秘密鍵でべき乗根を求める。復号には、第1の秘密鍵との乗算、第2の秘密鍵での置換操作、第3の秘密鍵の多項式との乗算、べき乗数等を示す第4の秘密鍵でべき乗根を求めることが必要で、第4の秘密鍵を知らなければ、メッセージの各要素の複雑な多項式等の段階までしか暗号を破れないため、暗号の信頼性はさらに高い。

【0015】

請求項5の発明では、復号プログラムを情報ネットワークを介してデジタル情報処理装置に送信し、送信した復号プログラムで復号する。このため、復号プログラムの配布が容易になる。

【0016】

請求項6～8の発明では、この発明に適した復号装置や復号プログラムの記録媒体を提供し、特に請求項7の発明では、強固に暗号化した暗号をデコードできるので、暗号システムの安全性が特に高い。

【0017】

以上のように、この発明では新規な暗号化技術を元にして、それに対応した復号方法や復号装置等を提供するので、信頼性の高い暗号システムを構築できる。

【0018】

【実施例】

図1～図6に実施例を示す。予め主な記号を説明すると、 $GF(2^k)$ 、 $GF(2^n)$ はガロワ体を表す。用いる体の素体としては標数 p (p は素数)のガロワ体の他に、標数が0の体、即ち有理数体 Q 等でも良い。標数 p は素数あるいは0とする

が、デジタル情報処理装置での処理の便宜のために、2が好ましい。ガロワ体 $GF(2^k)$ 、 $GF(2^n)$ は素体の有限次元拡大体の例で、 k の値は例えば 64 ~ 16384 程度とし、実施例では 1024 を想定する。 n の値は例えば $2k$ 程度とし、128 ~ 32768 程度として、実施例では 2048 を想定する。

【0019】

$F(X)$ はガロワ体 $GF(2^k)$ の原始多項式で、 k 次の多項式であり、同様に $H(X)$ はガロワ体 $GF(2^n)$ の原始多項式で、 n 次の多項式であり、復号を容易に行うため、 $F(X)$ や $H(X)$ は原始多項式が好ましい。しかし $F(X)$ はガロワ体 $GF(2^k)$ の単なる既約多項式でもよく、同様に $H(X)$ はガロワ体 $GF(2^n)$ の単なる既約多項式でも良い。 α は多項式 $F(X)$ の根の 1 つであり、 $F(\alpha) = 0$ となる。 γ は $H(X)$ の原始根の 1 つで、 $H(\gamma) = 0$ であり、 x は自然数で、 γ^x はガロワ体 $GF(2^n)$ の 0 でない元である。

【0020】

M はメッセージを意味し、実施例では 1024 ビット長のデータで、1024 個の要素 $m_1 \sim m_k$ (例えば $k = 1024$) からなるベクトルと見なすことができ、ガロワ体 $GF(2^k)$ の元である。この明細書で、自然数の集合 N は 0 及び正の整数の集合とする。暗号化のアルゴリズムでは、 t 個の多項式、(いずれもガロワ体 $GF(2^k)$ の元)、 $\beta_1(\alpha)$ 、 $\beta_2(\alpha)$ 、 \dots 、 $\beta_t(\alpha)$ を用い、

$$M(\alpha) = M \beta_1(\alpha) \cdot M \beta_2(\alpha) \cdot \dots \cdot M \beta_t(\alpha) \mod F(\alpha) \quad (1)$$

に従って、メッセージ M を第 1 段の暗号 $M(\alpha)$ に変換する。 $M(\alpha)$ を、メッセージ対応部と呼ぶ。また $\beta_1(\alpha) \sim \beta_t(\alpha)$ の積を単に β と呼ぶ。式 (1) 等の演算はガロワ体上の演算であり、 $F(\alpha)$ での剰余を問題にしていることは明らかなので、文脈から明らかな場合、剰余演算を行っていることを明記しない場合がある。

【0021】

$n - k$ 次元 (例えば 1024 次元で、実施例では 1024 ビット長) のノイズ $r(\alpha)$ を用意し、メッセージ対応部 $M(\alpha)$ の末尾などに付加し、これに対称群 (置換群) の元を作用させて、メッセージ対応部 $M(\alpha)$ の各要素とノイズ $r(\alpha)$ の各要素の順序を置換し、要素を互いにシャッフルしたものを Γ とする。 Γ は n 次元のデータで、ガロワ体 $GF(2^n)$ の元である。 $M(\alpha)$ から Γ への写像を Φ^{-1}_{nk} 、

復号時に使用する $\Phi^{-1}nk$ の逆写像を Φnk とする。 $M(\alpha)$ と Γ との間の変換を、暗号化か復号かを区別せずに、置換と呼び、暗号化を意味するか、復号を意味するかは、文脈により指定する。

【 0 0 2 2 】

Γ に γ^x を乗算すると、得られる多項式 C の各次元の係数は、ノイズに由来するものとメッセージに由来するものとが入り交じった多項式となる。多項式 C を各次元の要素 C_i の集合として表記すると $C = \{C_i(M)\}$ となる。この C が暗号で、メッセージ M の関数であることを強調する場合、暗号 C を $C(M)$ と表記する。

【 0 0 2 3 】

以上に暗号化のアルゴリズムを示したが、暗号化は実用的にはアルゴリズムを伏してより簡便に行う。公開鍵として、 $C(X) = \{C_i(X)\}$ を公開し、公開鍵の X に M を代入すると、メッセージ M の各要素 ($m_1 \sim m_k$) の多変数の多項式として各 $C_i(M)$ が定まり、これを暗号とする。

【 0 0 2 4 】

秘密鍵は、 $F(X)$, $H(X)$, x (あるいは γ^x), Φnk , β , t で

$$\beta = \beta_1(\alpha) \cdot \beta_2(\alpha) \cdot \dots \cdot \beta_t(\alpha) \quad (2)$$
 で、 t は 1 以上の自然数である。 γ が原始根の場合、ガロワ体 $GF(2^n)$ の任意の 0 でない元は、 γ^{-x} と表現でき、原始根のべき乗との乗算は容易である。 f は M^t からべき乗根 M を求めるための自然数 (乗数) で、 t が $2^k - 1$ と素なら、このような f が存在する。このことから、 $(t, 2^k - 1)$ は 1 が好ましい。なお (a, b) は、 a , b の最大公約数を意味する記号である。

【 0 0 2 5 】

以下で、ネットワークは情報ネットワークを意味するものとし、デジタル情報処理装置はコンピュータや、論理回路を内蔵した暗号通信用のチップ等を意味するものとする。記録媒体は、コンピュータや復号用のチップ等で読み取り可能なものとする。

【 0 0 2 6 】

図 1 に、暗号化装置 4 と復号装置 6 との接続を示すと、これらはインターネッ

ト等のネットワークにより接続され、暗号化装置 4 は、復号装置 6 側に設けた公開鍵記憶部 8 から、公開鍵 $C(X)$ を入手して、平分作成部 2 で作成したメッセージ M を暗号化する。メッセージ M はガロワ体 $GF(2^k)$ の元である。メッセージ M の構成は (m_1, m_2, \dots, m_k) で、 k ビット長であり、公開鍵 $C(X)$ を用いた暗号 $C(M)$ への暗号化では、 n 次元の公開鍵 $C(X)$ の各要素 $C_i(X)$ に対して ($i = 1 \sim n$)、 X にメッセージ M を代入する。この結果、得られる暗号 $C(M)$ はガロワ体 $GF(2^n)$ の元となる。

【 0 0 2 7 】

復号装置 6 側には秘密鍵記憶部 10 があり、ガロワ体 $GF(2^k)$ の原始多項式 $F(X)$ 、ガロワ体 $GF(2^n)$ の原始多項式 $H(X)$ 、ガロワ体 $GF(2^n)$ の原始根 γ の値 (原始根が複数ある場合) と、そのべき乗 γ^x の x 、ノイズとメッセージ対応部とを分離するための対称群の元 Φ_{nk} 、メッセージ M をガロワ体 $GF(2^k)$ 内で多項式と乗算した際の多項式 β 、並びに多項式 β との乗算に伴いメッセージ M を t 乗した際の t 等が記憶されている。

【 0 0 2 8 】

12 は乗算処理部で、暗号 $C(M)$ にガロワ体 $GF(2^n)$ の元 γ^{-x} を乗算し、 Γ に変換する。14 は置換処理部で、 Γ に対称群の元 Φ_{nk} を作用させ、メッセージ対応部 $M(\alpha)$ とノイズとに分離し、メッセージ対応部 $M(\alpha)$ を取り出す。16 は第 2 の乗算処理部で、メッセージ対応部 $M(\alpha)$ に、多項式 β の逆元 β^{-1} を乗算し、メッセージ M の t 乗を求める。そしてメッセージ M の t 乗に対して、適宜の自然数 f でべき乗して、メッセージ M に復号する。このような f は、 t が $2^k - 1$ と素であれば存在する。

【 0 0 2 9 】

図 2 に、暗号化のアルゴリズムを示す。メッセージ M 、(例えば 1024 ビット長のデータで、メッセージ M 内に既にノイズを含んでいても良い)、をガロワ体 $GF(2^k)$ の元とし、式 (1)

$$M(\alpha) = M\beta_1(\alpha) \cdot M\beta_2(\alpha) \cdot \dots \cdot M\beta_t(\alpha) \mod F(\alpha) \quad (1)$$

により処理して、メッセージ対応部 $M(\alpha)$ とする。メッセージ対応部 $M(\alpha)$ を $k - 1$ 次以下の多項式と見なすと、各係数にはメッセージ M の各要素 $m_1 \sim m_k$ が複

雑に入り交じり、 $m_1 \sim m_k$ の t 次の多項式と見なすことができる。メッセージ対応部 $M(\alpha)$ を単独で用いた場合の暗号の信頼性は確認されておらず、以下の手続きで暗号を補強する。

【 0 0 3 0 】

メッセージ対応部 $M(\alpha)$ を $n - k$ 次元のノイズ $r(\alpha)$ とシャッフルする。このシャッフルは、例えばメッセージ対応部 $M(\alpha)$ の末尾にノイズ $r(\alpha)$ を付加し、これに対称群の元 Φ^{-1}_{nk} を作用させて、ガロワ体 $GF(2^n)$ の元 Γ に変換するものである。

【 0 0 3 1 】

続いて Γ に γ^x を乗算し、ノイズ $r(\alpha)$ の各成分とメッセージ対応部 $M(\alpha)$ の成分を、ガロワ体 $GF(2^n)$ での多項式表現の各次数において、複雑に入り交じらせる。ここに γ は原始多項式 $H(X)$ の原始根で、 x の値を選ぶことにより、ガロワ体 $GF(2^n)$ の 0 以外の任意の元を、 γ^x として表現することができる。この結果、得られた暗号 C は極めて強固なものとなる。

【 0 0 3 2 】

なおここで暗号化には、式(1)による処理と、ノイズ $r(\alpha)$ の付加と置換（シャッフル）、並びに γ^x の乗算の 3 段階の手続きを行ったが、これらはこの順に行う必要はない。例えば最初にメッセージ M とノイズ r とのシャッフルを行った後に、多項式との乗算や原始根のべき乗との乗算を行っても良く、あるいは最初に原始根のべき乗との乗算を行った後に、ノイズとのシャッフルを行い、最後に多項式との乗算を行っても良い。また実施例での暗号の信頼性は極めて高いので、上記の 3 手続きに代えて、ノイズの付加並びにシャッフル、及び多項式との乗算もしくは原始根のべき乗との乗算のいずれか一方を行っても良い。

【 0 0 3 3 】

暗号化のアルゴリズムを図 2 に示したが、実際の暗号化では送信者に暗号化のアルゴリズムを知らせる必要はない。実際の暗号化では、図 3 に示すように、公開鍵 $C(X)$ として、メッセージ M と同じ長さの不定元 X を用い、 X の多項式として公開鍵の各要素 $C_i(X)$ ($i = 1 \sim n$) を公開する。送信者は、不定元 X にメッセージ M を代入すれば、暗号 $C(M)$ が得られる。従って暗号化は極めて容易で

あり、かつ公開鍵 $C(X)$ は強い 1 方向性の関数である。

【 0 0 3 4 】

図 4 に復号のアルゴリズムを示す。復号装置 6 で受信した暗号 $C(M)$ に対し、 γ^{-x} を乗算し、 Γ を求める。 γ^{-x} はガロワ体 $GF(2^n)$ の元であり、この乗算は容易である。次いで Γ にノイズの付加と置換とに用いた写像 Φ^{-1}_{nk} の逆置換から成る写像 Φ_{nk} を施し、 Γ をメッセージ対応部 $M(\alpha)$ へと変換し、ノイズ $r(\alpha)$ を除去する。この過程で、ガロワ群の元の数 2^n から 2^k へと減少する。続いてメッセージ対応部 $M(\alpha)$ に対して、式 (1) で用いた t 個の多項式 $\beta_1(\alpha) \sim \beta_t(\alpha)$ の積 β の逆元を乗算し、 $M(\alpha)$ を M^t に変換する。ここで t と $2^k - 1$ とが素であれば、適当な自然数 f が存在して、 $M^{tf} = M$ となり、これからメッセージ M を求めることができる。

【 0 0 3 5 】

図 5 に、復号プログラムのネットワーク 24 を介しての配布を示す。20 は配信者で 22 は、受信者で、例えば適当な秘密鍵等を用いて、受信者 22 は配信者 20 に対して復号プログラムの送信を要求し、これに対応してネットワーク 24 を介して復号プログラムを配布する。配布送信する復号プログラムは、図 4 のアルゴリズムを実現したものである。

【 0 0 3 6 】

図 6 に、暗号装置 30 の例を示すと、32 は入出力で、外部との通信や外部のコンピュータ等との接続に用い、34 は公開鍵記憶部で、公開鍵 $C(X)$ を記憶して公開し、36 は乗算処理部で γ^{-x} を乗算し、 γ^{-x} の値は乗算処理部 36 で記憶しているものとする。38 は置換処理部で、 Γ をメッセージ対応部 $M(\alpha)$ へ変換するための対称群の元を記憶して、 Γ を $M(\alpha)$ に変換し、40 は乗算処理部で、多項式 β^{-1} を記憶して、メッセージ対応部 $M(\alpha)$ を M^t と乗算する。42 は f 乗処理部で、 M^t をさらに f 乗して、メッセージ M へと復号する。44 は暗号化部で、暗号装置 30 側で作成したメッセージ M を暗号化するためのものである。なおこれらの処理部 36 ~ 44 は、レジスタと論理ゲート等の組み合わせ等により容易に実現でき、あるいはまたソフトウェアをコンピュータに搭載しても実現できる。

【 0 0 3 7 】

実施例は公開鍵暗号として用いる場合を示したが、秘密鍵暗号として用いても良く、その場合、秘密鍵の原始多項式や x の値、ノイズとのシャッフルに用いた対称群の要素 Φ_{nk} 、多項式 β 、 t の値、あるいは M の長さ等を適宜に更新すれば、極めて寿命の長い暗号システムが得られる。実施例は特定の処理を示したが、これらと等価な処理はこの発明に含まれ、例えば各秘密鍵は文字通りに秘密鍵を記憶する必要はなく、秘密鍵と等価、もしくは秘密鍵に変換可能なものであればよい。

【図面の簡単な説明】

- 【図 1】 実施例での暗号化装置と復号装置との接続を示すブロック図
- 【図 2】 実施例での暗号化アルゴリズムを示すフローチャート
- 【図 3】 実施例での暗号化処理を示すフローチャート
- 【図 4】 変形例での復号アルゴリズムを示すフローチャート
- 【図 5】 実施例での復号プログラムの配信を示す図
- 【図 6】 実施例での復号装置の構成を示すブロック図

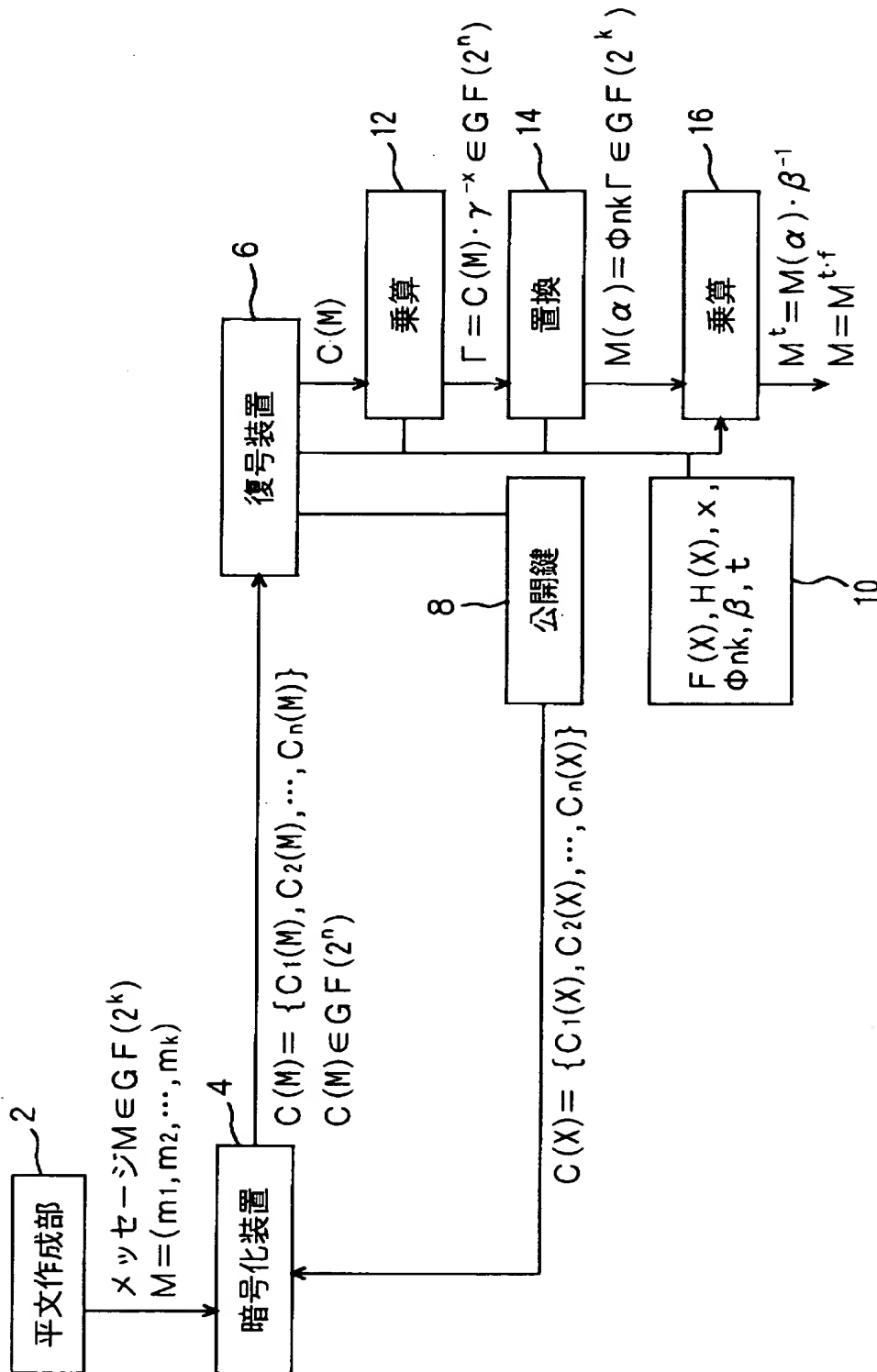
【符号の説明】

- 2 平分作成部
- 4 暗号化装置
- 6 復号装置
- 8 公開鍵記憶部
- 1 0 秘密鍵記憶部
- 1 2 乗算処理部
- 1 4 置換処理部
- 1 6 乗算処理部
- 2 0 配信者
- 2 2 受信者
- 2 4 ネットワーク

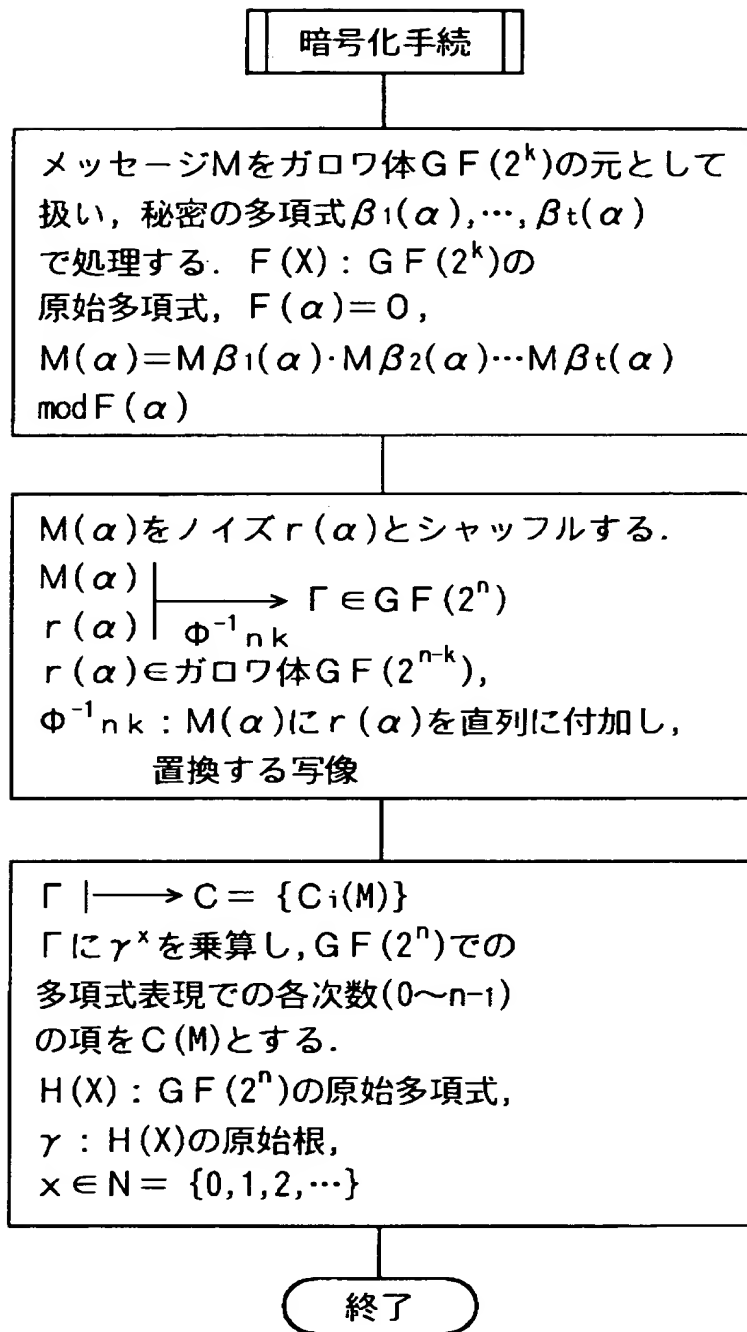
3 0	暗号装置
3 2	入出力
4 4	暗号化部
3 6	乗算処理部
3 8	置換処理部
4 0	乗算処理部
4 2	f 乗処理部
4 4	暗号化部

【書類名】 図面

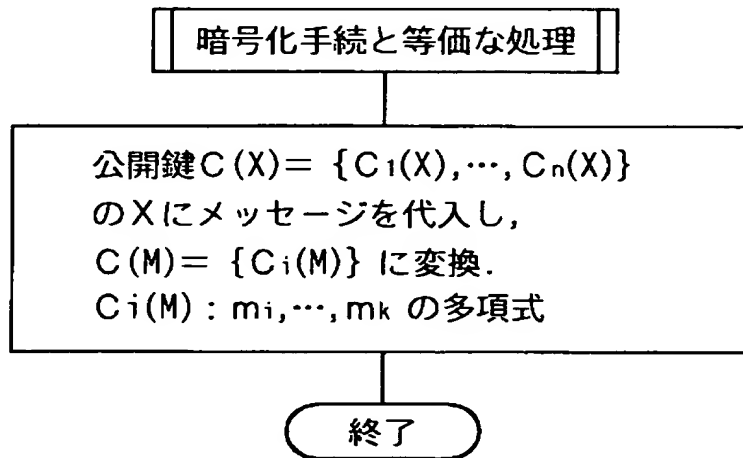
【図 1】



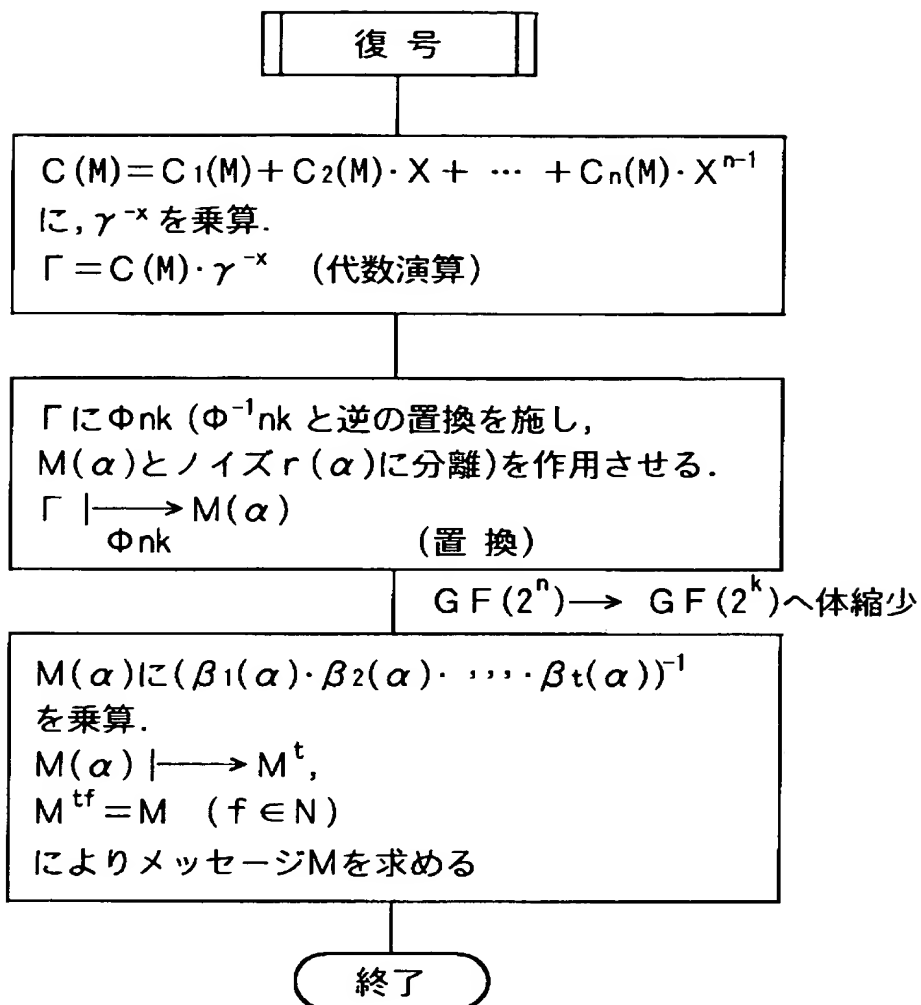
【図 2】



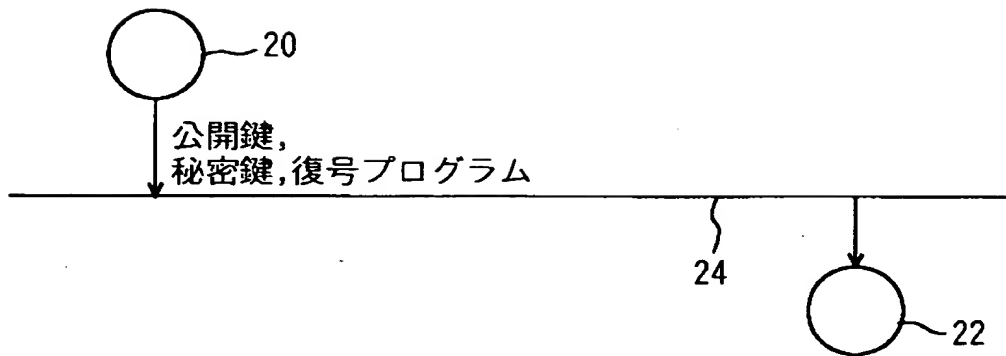
【図 3】



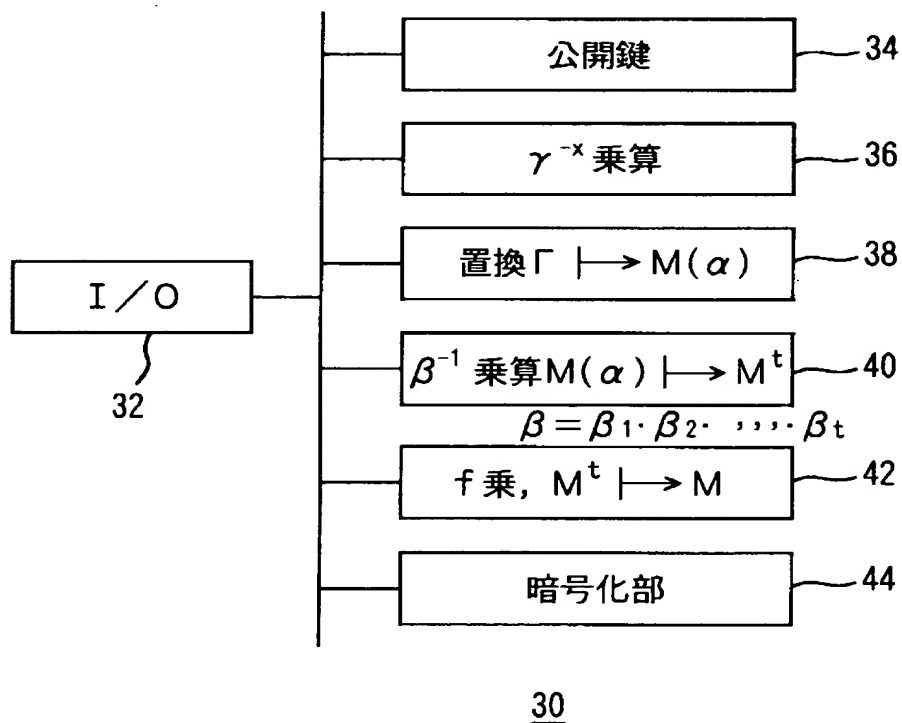
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【構成】 メッセージ M をガロワ体 $GF(2^k)$ の元 (m_1, m_2, \dots, m_k) と見なして、 M に多項式 $\beta_1(\alpha) \sim \beta_t(\alpha)$ を乗算し、

$$M(\alpha) = M\beta_1(\alpha) \cdot M\beta_2(\alpha) \cdot \dots \cdot M\beta_t(\alpha)$$

を求める。 $M(\alpha)$ に直列に $n - k$ 次のノイズベクトル $r(\alpha)$ を付加して、 n 次元に拡張し、置換操作を施して、 Γ に変換する。 Γ にガロワ体 $GF(2^n)$ の元 γ^x (γ はガロワ体 $GF(2^n)$ の乗法群の原始根)を乗算し、暗号 $C(M)$ とする。実用的には暗号 $C(M)$ は、公開鍵 $C(X)$ の X にメッセージ M を代入することで求められる。暗号 $C(M)$ に γ^{-x} を乗算し、逆の置換操作を施して、ノイズベクトル $r(\alpha)$ を分離し、 $\beta_1(\alpha) \sim \beta_t(\alpha)$ の逆元を乗算し、適当にべき乗して M に復号する。

【効果】 多変数の多項式を用いた強固な暗号システムを提供できる。

【選択図】 図 1

認 定 ・ 付 加 情 報

特許出願の番号	特願 2 0 0 0 - 0 6 6 2 2 6
受付番号	5 0 0 0 0 2 8 6 0 5 2
書類名	特許願
担当官	第八担当上席 0 0 9 7
作成日	平成 1 2 年 4 月 2 0 日

< 認定情報・付加情報 >

【提出日】	平成12年 3月10日
-------	-------------

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 6 2 9 7]

1. 変更年月日	1 9 9 0 年 8 月 7 日
[変更理由]	新規登録
住 所	京都府京都市南区吉祥院南落合町 3 番地
氏 名	村田機械株式会社

出 願 人 履 歴 情 報

識別番号 [5 9 7 0 0 8 6 3 6]

1. 変更年月日	1 9 9 7 年 1 月 2 1 日
[変更理由]	新規登録
住 所	大阪府箕面市栗生外院4丁目15番3号
氏 名	笠原 正雄